130.00 - 122 DAC

#6

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Shuang Ji and Eva Chen
SERIAL NO:	08/533,706
FILED:	September 26, 1995
TITLE:	VIRUS DETECTION AND REMOVAL APPARATUS FOR COMPUTER NETWORKS
EXAMINER:	To be assigned
GROUP ART UNIT:	2413
ATTY.DKT.NO.:	2124

"Express Mail" mailing label number EM145206943US

Date of Deposit 2 July 1996

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner For Patents, Washington, D.C. 20231.

Joy S. Allender

JAllender
Signature

ASSISTANT COMMISSIONER FOR PATENTS
BOX DAC
WASHINGTON, D.C. 20231

PETITION TO MAKE SPECIAL

Sir:

Petition and Fee

Pursuant to 37 C.F.R. §1.102, and consistent with the procedural requirements outlined in M.P.E.P. §708.02 (VIII), Applicant hereby petitions to make the above identified patent application special. Accompanied herewith is the petition fee of $130.00 as set forth in 37 C.F.R. §1.17(i).

Single Invention Statement

Applicant asserts that, although each of the claims in the above-identified application are mutually patentably distinct, all of the claims in the above-identified application are directed to a single invention for detecting viruses in data transfers. If the Office determines that all the claims presented are not obviously directed to a single invention, Applicant will make an election without traverse as a prerequisite to the grant of special status.

Pre-Examination Search

Applicant asserts that a pre-examination search was conducted by a professional searcher at the U.S. Patent and Trademark Office. The search covered: (1) Class 364, Subclasses 274.2, 276.6, 286.4 and 944.9; and (2) Class 395, Subclasses 183.04 and 183.15. The search resulted in identification of the following U.S. Patent documents:

1. U.S. Patent No. 4,975,950 issued to Lentz;
2. U.S. Patent No. 5,319,776 issued to Hile et al.;
3. U.S. Patent No. 5,414,833 issued to Hershey et al.;
4. U.S. Patent No. 5,440,723 issued to Arnold et al.;
5. U.S. Patent No. 5,444,850 issued to Chang;
6. U.S. Patent No. 5,448,668 issued to Perelson et al.;
7. U.S. Patent No. 5,452,442 issued to Kephart;
8. U.S. Patent No. 5,485,575 issued to Chess et al.;
9. U.S. Patent No. 5,491,791 issued to Glowny et al.;
10. U.S. Patent No. 5,511,163 issued to Lerche et al.

A copy of each of these references is enclosed herewith.

Detailed Discussion of the Identified References

The claimed features of Applicant's invention facilitate efficient and expansive virus detection and removal by providing such detection and removal in data transfers such as between first and second computers. Data to be transferred is transmitted or communicated to a server. The server scans the data for a virus, specifies remedial actions in the event of virus detection, and selectively transfers the data dependent upon the presence of a virus in the data.

The claimed subject matter is patentably distinguishable over the references identified in the pre-examination search since they do not disclose or suggest the features recited in Applicant's claims.

Detailed discussions of these references are provided below. These discussions point out, with the particularity required by 37 C.F.R. §1.111(b) and (c), how the claimed subject matter is distinguishable over the references.

U.S. Patent No. 4,975,950 issued to Lentz

The Lentz reference apparently discloses a system and method for preventing the alteration of stored data by a computer virus by checking for a virus during the initialization (e.g. power up or reset) of a computer system. A device takes control of the central processing unit before boot up by preventing the transfer of control to boot up files, checks the system files for viruses, and generates an alarm signal if a virus is detected.

Applicant's claimed invention is distinguishable over Lentz. While Lentz may generally detect computer viruses, there is no detection of such viruses in a data transfer. Rather, Lentz merely checks files existing on a computer system after the power is turned on or the system is reset. Thus, there is no transmission or communication of data to be transferred in Lentz. Similarly, there is clearly no server for receiving the data to be transferred, for determining whether the data to be transferred contains a virus and for selectively transferring the data dependent upon the existence of a virus.

Accordingly, Lentz does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,319,776 issued to Hile et al.

The Hile et al. reference apparently discloses the detection of viruses in transit between source and destination media wherein an input data stream is tested using a finite state machine capable of testing against multiple search strings representing the signatures of multiple known viruses. For example, viruses may be detected in a computer system with a hard disk 24b, CPU 18b, and RAM 20 connected to a bus 16. Data input through the serial port of the computer system is placed in a buffer 30 in the RAM 20. Preloaded finite state tables 34 are provided with data for comparison to the sequence of incoming data character by character to detect a virus signature string while the sequential data is in the computer's buffer 30.

Thus, Hile et al. discloses a buffer for storing a string of data while it is being compared to predetermined strings to detect viruses.

By contrast, Applicant's claimed invention facilitates the selective transfer of data using a server which is arranged to scan the data for a virus and, additionally, specify data handling actions dependent upon the existence of a virus. By including such virus scanning and data handling actions in a server, Applicant's claimed invention prevents the spread of viruses in data transfers which are routed through the server such as those between a first computer outside of a network and a second computer within the network. Hile et al., however, merely scans data strings in the memory buffer of a computer which is the source or destination for data.

Accordingly, Hile et al. does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,414,833 issued to Hershey et al.

The Hershey et al. reference apparently discloses a network security agent. As shown in Figure 3, the security agent 10 and communicating devices 40, 41 are connected to a bit stream so that the security agent 10 can search for characteristic sequential patterns in data traversing the network medium. A finite state machine array is used to detect virus signature patterns. For example, a first state machine may be arranged to continuously analyze bits in the data stream, and where a matching sequence is found, additional state machines in the array may be initiated to provide parallel data pattern analyses (see, e.g.

col. 9, line 62 through col. 10, line 40 as well as Figures 1A-F and 2 and their related description).

The Hershey et al. device continuously observes the bit stream traversing a local network medium to look for viruses within the network. Thus, the device is merely reactive to viruses which have already entered, and possibly permeated, the network. Additionally, since the device merely observes the stream of data and does not concern or participate in data transfers, its remedies include only reactive types such as alarms or messages indicating the potential presence of a virus.

By contrast, Applicant's claimed invention provides for the detection and selective removal of viruses in data transfers by communicating or transmitting the transferred data to a server, determining whether the data contains a virus at the server, performing data handling actions on the transferred data where a virus is detected, and selectively allowing the transfer of the data to a destination based upon the presence of a virus in the data. Since Applicant's claimed invention can selectively stop completion of a transfer based upon the detection of a virus, it can prevent the virus from ever penetrating a network (or permeating, where an intranetwork transfer is routed through the server, or leaving, where the destination is outside of a network). Moreover, since the server participates in the transfer of data, a variety of virus detection techniques may be implemented in addition to signature scanning such as emulation. Additionally, again because the server participates in the transfer of data, remedies such as removal of the virus from the affected file may be undertaken so that clean data may be exchanged to or from a computer on the network.

Accordingly, Hershey et al. does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,440,723 issued to Arnold et al.

The Arnold et al. reference apparently discloses the detection of viruses in a digital data processing system by looking for anomalous behavior by monitoring patterns of activity in computational processes or changes in executable files. When anomalous behavior is detected, the informational state history of the digital data processing system is scanned to see whether the virus that is causing the behavior is known so that remedial action may be taken. If the virus is not known, then an identifying signature is extracted from the unknown virus and stored to enable future detection. Where the infected computer is part of a network, "neighbor" computers (those which the infected computer frequently communicates with) may be informed in lieu of every computer in the network to conserve resources.

Basically, Arnold et al. is a method of monitoring a computer's behavior to detect the presence of a virus, scanning the computer for known viruses and identifying new viruses. As applied to the potential spread of viruses, particularly to computers in networks, Arnold et al. merely informs selected "neighboring" systems as to the existence of a virus. Thus, Arnold et al. clearly does not disclose or suggest the detection of viruses in a data transfer, particularly where the data to be transferred is communicated to a server, where the virus is detected and treated at the server, and where the transfer is selectively completed based upon the presence of a virus in the transferred data. The only apparent disclosure of avoiding the spread of viruses - informing neighboring computer systems that a virus was detected on a first computer system - is reactive, speculative and clearly divergent from Applicant's claimed invention.

Accordingly, Arnold et al. does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,444,850 issued to Chang

The Chang reference apparently discloses preboot control of a workstation on a network. Prior to loading the workstation operating system software during the boot sequence, the workstation may be accessed and controlled by using the basic input/output system (BIOS) of the workstation. BIOS access allows the server to communicate with the workstation and the server management application (SMA) software is arranged to perform various preboot functions. For example, virus detection and repair may be applied to workstation hard disk boot sectors prior to executing the boot sequence.

The Chang reference is directed towards remote access of an individual workstation prior to execution of the boot sequence so that an administrator can perform certain management functions without requiring physical access to each workstation. By contrast, Applicant's claimed invention facilitates the detection and removal of viruses in data transfers. Because of such clear divergence, Chang does not disclose or suggest detection and removal of a virus in a data transfer wherein a server receives the transferred data, scans it, and selectively allows transfer based upon the existence of a virus in the data to be transferred. Rather, the only apparent reference to virus detection in Chang is to those residing in workstation hard disk boot sectors rather than in data which is being transferred from one place to another through a server.

Accordingly, Chang does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,448,668 issued to Perelson et al.

The Perelson et al. reference apparently discloses probabilistic detection of viruses in an original computer file by generating a protection file and comparing the original file to the protection file to detect changes. The protection file may be generated by using a computer to provide random test strings and comparing the test strings to the original file so that non-matching strings may be added to the protection file. A file may then be tested for changes by determining whether a match exists between any of the test strings in the protection file and the tested file. A match indicates a change in the tested file. In a network as shown in Figure 3, since each protection file is created based upon test strings which are randomly generated by each different computer, a variety of protection files would be presented by the computers in the network. Thus, in a network an expanded database for the detection of viruses is provided.

Perelson et al. is directed towards techniques for detecting viruses by expanding upon the comparison data. Therefore, there is no disclosure or suggestion of detecting and selectively removing viruses in data transfers. Likewise, there is no disclosure or suggestion of communicating the transferred data to a server, scanning and handling the data using the server, and selectively transferring the data depending upon the existence of viruses in the data being transmitted.

Accordingly, Perelson et al. does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,452,442 issued to Kephart

The Kephart reference apparently discloses statistical virus signature extraction and the evaluation of virus signatures. A virus is examined to identify an overall sequence of bytes which is unlikely to vary. Candidate computer virus signatures are then derived from the overall sequence of bytes by extracting several "n-grams" from the sequence. The extracted and derived virus signatures (or previously established signatures) may be evaluated by estimating the probability that the signature will occur in computer programs which will be executed on a processor to be monitored. This probability is analyzed relative to a threshold so that sequences which would produce false positive virus indications are not used by the virus scanner.

Thus, Kephart is directed towards improved detection of computer viruses on a computer system such as a single personal computer by modifying the reference data to which suspect files are compared so that false positives are avoided. By contrast, Applicant's claimed invention is for detecting and selectively removing viruses in data transfers. There is no apparent disclosure in Kephart of the detection of viruses in data transfers. Similarly, there is no disclosure or suggestion of communicating transferred data to a server, scanning the data, taking remedial action, and selectively transferring the data based upon the existence of a virus in the transferred data.

Accordingly, Kephart does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,485,575 issued to Chess et al.

The Chess et al. reference apparently discloses the analysis of the structure and host attachment means of a virus to characterize the virus. The virus is characterized so that it may be subsequently detected by a virus scanner. For example, to characterize the virus, an infected program and a corresponding original may be obtained, a description of how the virus attaches to host programs may be generated, a variety of virus samples may be analyzed to find portions which do not vary, and variable regions of the virus may be located.

The Chess et al. reference discloses the analysis of a virus so that it may be more easily and accurately detected and repaired in subsequent virus scans. Thus, there is no apparent disclosure or suggestion of detecting and selectively removing viruses in data transfers or, likewise, communicating transferred data to a server, scanning the data, taking remedial action, and selectively transferring the data based upon the existence of a virus in the transferred data.

Accordingly, Chess et al. does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,491,791 issued to Glowny et al.

The Glowny et al. reference apparently discloses remote workstation inventorying and monitoring within a distributed computing environment comprising a plurality of workstations interconnected by a network. A non-server work station is designated as the monitor. The monitor work station generates an execute command and each remote work station to which the execute command is directed executes a diagnostic routine. The diagnostic routine provides information about the workstation which may be compiled into the form of a report file which may be returned to the monitor work station for analysis and, possibly, issuance of an alarm.

This reference is apparently directed towards facilitating remote management and maintenance of the workstations in a local area network so that the network administrator does not have to manually correct workstation problems or continually reconfigure workstation settings which are altered by users. By contrast, Applicant's claimed invention facilitates the detection and removal of viruses in data transfers. The only apparent disclosure of virus detection in the reference is that when a workstation is remotely monitored and inventoried, it may also be scanned for viruses. Clearly, then, there is no detection of viruses in a data transfer, nor is there communication of the data to be transferred to a server, scanning and remedial action at the server, or selectively transferring the data depending upon the ongoing existence of a virus in the data.

Accordingly, Glowny et al. does not disclose or suggest Applicant's claimed invention.

U.S. Patent No. 5,511,163 issued to Lerche et al.

The Lerche et al. reference apparently discloses the detection of certain viruses after their introduction into a network. Specifically, a workstation 8 within the network is connected to receive information on the network 1 through the use of a network adapter 7 which is arranged to receive data traversing the network. The workstation 8 receives and signature scans certain data to detect viruses. An alarm or, where applicable, a vaccine for a detected virus may be sent to a plurality of personal computers 2 on the network in response to network permeation by the virus.

Lerche et al. observes the bit stream traversing local network media to look for viruses within the network and reacts to the presence of a virus where one is detected in the bit stream. Since the Lerche et al. device taps into the local network media, it only detects viruses which have already penetrated the network and attempts to remedy the infection by notifying users or sending out a vaccine if it is available (thus, a troublesome virus for which a vaccine is unavailable can remain on several network computers untreated).

By contrast, Applicant's claimed invention detects viruses in data transfers by participating in and selectively allowing completion of the transfer of data through a server. Thus, for example, Applicant's claimed invention can clean viruses before their entry into a network and can selectively block a transfer into a network where a troublesome virus is detected. The data to be transferred is communicated to a server, and the server scans the data for viruses and takes remedial action if there is a virus. Thus, Applicant's claimed invention prevents the spread of viruses in data transfers which are routed through the server such as those between a first computer outside the server's network and a second computer inside the network. By contrast, Lerche et al. observes local network traffic and reacts only to viruses which have already entered the network by issuing alarms or vaccines to the affected parties.

Since Applicant's claimed invention prevents the spread of viruses in data transferred through the server, it can prevent the virus from ever penetrating the network. Moreover, since the server participates in the transfer of data, a variety of virus detection techniques may be implemented in addition to signature scanning such as emulation. Additionally, again because the server participates in the transfer of data, remedies such as removal of the virus from the affected file may be undertaken so that clean data may be exchanged to or from a computer on the network.

Accordingly, Lerche et al. does not disclose or suggest Applicant's claimed invention.

Conclusion

Applicant submits that the present petition satisfies all of the requirements of 37 C.F.R. §1.102. Favorable action is respectfully requested.

Respectfully submitted,
SHUANG JI and EVA CHEN

Dated: 2 July 1996 By:

Greg T. Sueoka
Registration No. 33,800
FENWICK & WEST
Two Palo Alto Square, Suite 600
Palo Alto, California 94306
(415) 858-7194